(12) UK Patent Application (19) GB (11) 2 297 017 (13) A

(43) Date of A Publication 17.07.1996

(21) Application No 9500532.8

(22) Date of Filing 11.01.1995

(71) Applicant(s)
Farncombe Technology Ltd

(Incorporated in the United Kingdom)

Telford Point, Telford Road, BASINGSTOKE, Hants, RG21 2XZ, United Kingdom

(72) Inventor(s)
Andrew Jim Kelley Glasspool

(74) Agent and/or Address for Service
Graham Jones & Company
77 Beaconsfield Road, Blackheath, LONDON, SE3 7LG, United Kingdom

(51) INT CL^6
H04N 7/167

(52) UK CL (Edition O)
H4R RPTS R22V
U1S S2204 S2209

(56) Documents Cited
EP 0132401 A2 WO 94/13081 A1 US 4944006 A
US 4916737 A US 4388643 A

(58) Field of Search
UK CL (Edition O) H4R RPTS
INT CL^6 H04N
Online: WPI, JAPIO, INSPEC

(54) Encryption of television services

(57) Transmitting a single control word for a plurality of differently scrambled services enables much simpler encoding equipment to be used. A random number from a generator 1 is encrypted using respective session keys to derive control words cw1, cw2., used to scramble a respective service. The random number is also transmitted to a decoder 3 where the control words cw1, cw2., are derived by encrypting of the random number with the session keys sk1, sk2., stored at the decoder. In a preferred arrangement, the session keys are replaced by a common operating key modified by entitlement data which differs from service to service. The compression of TV services often relies upon the transmission of a TV frame, in compressed form and then the difference between that frame and the next frame. The image data and the difference image data are encrypted to different extents to enable partial viewing of an image by non subscribers.

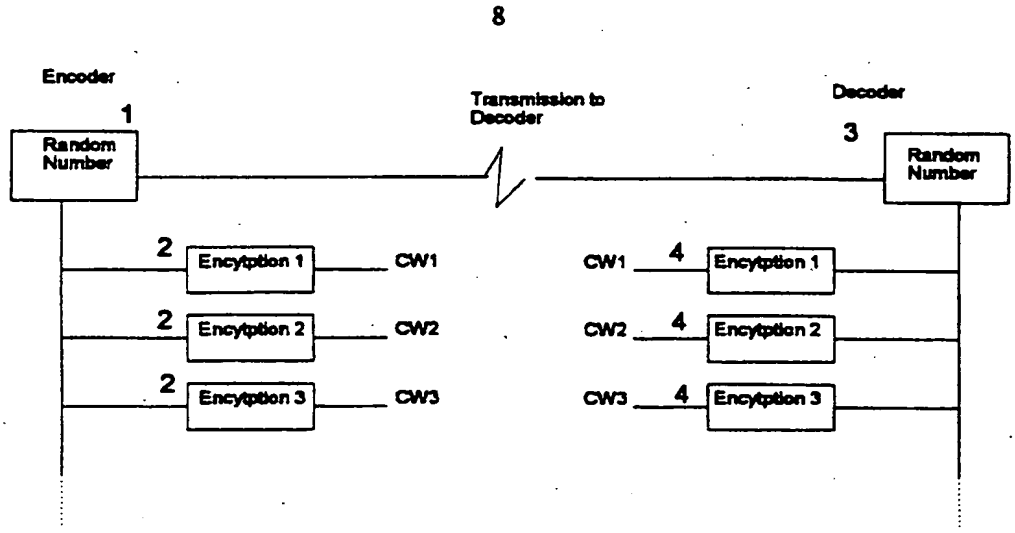

Figure 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 297 017 A

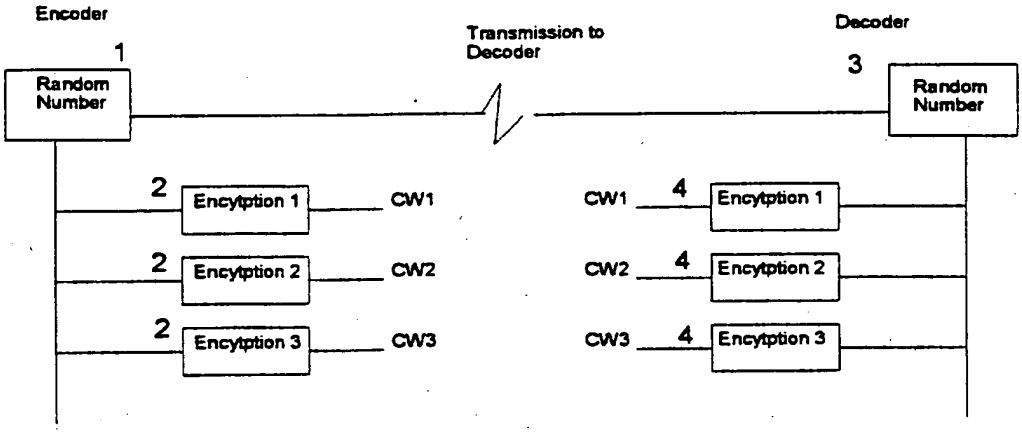
Encoder
1
Random Number
Transmission to Decoder
Decoder
3
Random Number
2
Encytption 1
CW1
2
Encytption 2
CW2
2
Encytption 3
CW3
CW1
4
Encytption 1
CW2
4
Encytption 2
CW3
4
Encytption 3

Figure 1

Encryption of Television Services

This invention relates to methods and apparatus for encrypting and decrypting television services.

Digital compression allows the transmission of multiple television (video, audio and possibly data) services within the RF bandwidth that a single video service occupies. Thus one cable RF channel may carry 10 television services. Compression of video, audio and data in this way allows for a television service to be transmitted down a conventional telephone line.

Each television service may be independently encrypted (or scrambled) so that it can be sold independently. It is expected, therefore, that at the transmission point that there will be the need to scramble hundreds or even thousands of services (e.g. 100 channel cable system, 10 TV services per channel).

Each service would normally be protected by a short life key of e.g. 64 bits, often referred to as a control word. The control word might be changed and the new one transmitted every 10 seconds (this period may vary from a few milliseconds upwards) in encrypted form. For 1000 services there would need to be 1000 control words. This control word would be decrypted in the decoder using another secret key (the session key) Sk, and then used for decrypting the television service. The session key may be different for each service that is protected.

The encryption equipment is expensive and the control of the encryption of so many channels could become complicated. The present invention relates to techniques

for limiting the encryption required and limiting the data required to control the encryption.

According to one aspect of the invention there is provided a method of transmitting television services, the method comprising independently encrypting each of a plurality of such services using respective control words, and transmitting common control data for all said services, whereby the common control data can be modified using respective key data for each said service to derive said respective control words for use in decrypting the respective services.

By using different session keys, the same encrypted control word may be used for each service since the result of the decryption will depend on the key Sk. Only those decoders that hold the correct key Sk for the service will be able to derive the correct control word. Transmitting a single control word for a plurality of differently-scrambled services enables much simpler encoding equipment to be used.

However in a practical decoder there may be one Sk applying to many services. The decoder will instead allow access to the service according to the state of a bit (a tier) in its memory. The tier represents the decoder's entitlement to the service; it may be time limited or it may be extended to include other data. The transmitted service may include identifying data which the decoder will compare with its stored entitlement data.

The decoder may therefore have the information to decrypt the service but will not do so unless it also holds the

corresponding entitlement. In this case, by "spoofing" the decoder into thinking it is decrypting one service when it is decrypting another, it will be possible to gain unauthorised access to services that were not intended to be decrypted by the decoder. Spoofing the decoder may be easy if many decoders operate in response to a single control word.

According to a preferred aspect of the invention, the decryption of the control word is performed using previously received entitlement data, which would differ from service to service. Thus for example if at the time the subscriber purchases a programme some secret data is transmitted to the decoder, possibly with the entitlement update, this secret data can be used to modify the control word that is generated for that service. Using this technique, it is no longer necessary to have different session keys for different services (although this is still possible if desired). Indeed it would be possible to eliminate the session key, although this is not preferred because for economy of data transmission it is preferred to have a relatively long session key modified by relatively short entitlement data.

Referring to the accompanying Figure 1, which schematically illustrates one example of a transmission technique according to the invention, in the encoder section a random number generator 1 generates a random number which is delivered to respective encryption blocks 2. In each encryption block, the random number is encrypted using a respective session key Sk1, Sk2, etc. to derive a respective control word CW1, CW2, etc. which is then used to scramble a respective service.

The random number is also transmitted to a decoder, where it is received at 3, and then delivered to one or more encryption blocks 4. The decoder stores the session key Sk for each service which it is authorised to de-scramble. Thus, the control word CW1, CW2, etc. for any of the services for which the session key Sk1, Sk2, etc. is held can be derived by encrypting the random number with the session key, thereby permitting de-scrambling of the respective service.

The random number is expected to be changed frequently, possibly once every 40 mS, but it may be valid for as long as, e.g., 10 seconds. The session keys may also be arranged to change frequently, in a predetermined way.

The encryption processes as shown in the figure may be replaced by decryption processes.

The preferred embodiment of the invention modifies the arrangement shown above in the following way. The session keys Sk1, Sk2, etc. are replaced by a common operating key K, but instead of using only this key in the encryption/decryption processes, the key is modified by entitlement data E which differs from service to service, to produce a modified operating key K'. If a subscriber purchases a service, they can be sent entitlement data possibly formed by a message containing a description of the service (possibly non-scrambled) and possibly some secret data in a message authenticated with a management key. This should be a unique description. A sequence number, the date or other period of validity is a typical method of achieving this. If secret data is needed it can be encrypted with the same management key that was used to authenticate the message and possibly to

send key K in the first instance. It is to be noted that the entitlement data isn't necessarily secret data; this is unnecessary if the data has to be authenticated with the management key. However, secret data improves the security of the system.

The entitlement data E is then used to modify the operating key K to derive K', which is then used for deriving the control word for the subsequently-transmitted service.

This approach means that it is no longer essential for the decoder to store many keys, and the amount of data required to be transmitted when services are differently-scrambled is very small.

In a preferred embodiment, the operating key K is arranged to change at frequent intervals in a known manner. The entitlement data E may be used to initialise the key K.

If a single control word is to be transmitted to cover all (or a plurality of) services on the RF channel there should be a means of synchronising the application of the control word. Since each service will operate at a different data rate we cannot synchronise the data transmission. Instead we can signal the change in control word; whenever it changes the next packet of data for that service should be encrypted under the new control word. The change in control word can be signalled in the data packets, for example by the modification of a bit from 1 - 0 - 1 - 0 etc. There are many schemes for achieving this type of synchronisation for a single service; they can easily be extended to

cover a group of services.

The main cost of encrypting a television service is the encryption of the data. In the MPEG compression standard it is proposed that there should be a block cipher used to encrypt/decrypt blocks of data. Each block of data may be treated independently or they may be linked to together by a technique referred to as cipher block chaining. Alternatively the data may be Xored with a psuedo-random binary sequence (PRBS) that is initialised by the control word. The PRBS would be reset every period.

The compression of TV services often relies upon the transmission of a TV frame, in compressed form, and then the differences between that frame and the next frame. For example a complete frame (I frame) may be sent every half a second (every 12 frames), the difference information being used to generate the intermediate frames. The difference information may refer to the previous or next I frame. In practice there may be many I frames, each one only applying to part of the complete TV frame at a time so that there are not discrete changes each time the whole I frame is updated.

According to another aspect of the invention (which may but is not necessarily combined with the aspect mentioned above) the image (or part-image) data on the one hand and the difference image data on the other hand are encrypted to different extents. One may be completely non-encrypted, or encrypted at a level or tier which permits viewing by a group of subscribers, whereas the other is encrypted to a higher extent.

The invention will be described in the context of the MPEG standard, where the image or part-image data is represented by I frames, but is applicable to other compression techniques.

If the I frames are encrypted, but none of the other data is encrypted it should not be possible to generate a TV picture. Thus the amount of data to be encrypted is significantly reduced, as is the cost of the encryption unit. The encryption may performed at the video service level where compression takes place, or at the transport layer in which case the encoder must know which packets contain I frames (or part of I frames). The decoder only needs to know which packets are encrypted.

If the I frames or part of the I frames are left in the clear and the remaining data is encrypted the broadcaster can offer a form of free preview since the picture would not be enjoyable, but it would be distinguishable. Clearly this could be extended to part of the I frame or a combination of the I frame and part of the difference information.

The present invention may be applied to services transmitted by cable or by other media. The invention extends not only to methods of transmission, but also to methods of reception, methods of encrypting and decrypting, and apparatus for encrypting, decrypting, transmission and reception of television services.

CLAIMS:

1. A method of transmitting television services, the method comprising independently encrypting each of a plurality of such services using respective control words, and transmitting common control data for all said services, whereby the common control data can be modified using respective key data for each said service to derive said respective control words for use in decrypting the respective services.

2. A method as claimed in claim 1, including the step of transmitting to selected decoders entitlement data which is used to determine at least part of said respective key data.

3. A method as claimed in claim 2, wherein the entitlement data is used to initialise key data which is arranged to change periodically.

4. A method as claimed in claim 2 or claim 3, wherein the entitlement data is used to modify key data which is common for a plurality of services.

5. A method as claimed in any preceding claim, wherein the television services are transmitted using compression techniques on a single channel.

6. A method of transmitting a television service in compressed form, by transmitting first data defining images or part images and second data defining changes to the images or part images defined by the first data, the method comprising encrypting the transmission, and controlling the encryption of data in dependence on whether the data is first data or second data.

7. A method as claimed in claim 6, wherein at least part of the first data is encrypted to a greater extent than at least most of the second data, thereby substantially to prevent viewing of any significant part of the service without decryption of the encrypted first data.

8. A method as claimed in claim 6, wherein at least part of the second data is encrypted to a greater extent than at least most of the first data, thereby to allow impaired viewing of the service without decryption of said encrypted second data.

The Patent Office

Application No: GB 9500532.8
Claims searched: 1 to 5

Examiner: Mr.SAT SATKURUNATH
Date of search: 3 April 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): H4R: RPTS

Int Cl (Ed.6): H04N

Other: Online: WPI, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0132401 A2	KABUSHIKI - see especially figures 3, 4, 6, 7, 12 and 16	1-4
X	WO 94/13081 A1	SCIENTIFIC - see especially figures 2-4	1-4
X	US 4944006	ZENITH - see especially figures 2, 3	1-4
X	US 4916737	TELEGLOBE - see especially figures 1, 2	1-4
X	US 4388643	NORTHERN - see especially figures 1, 2	1-4

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.